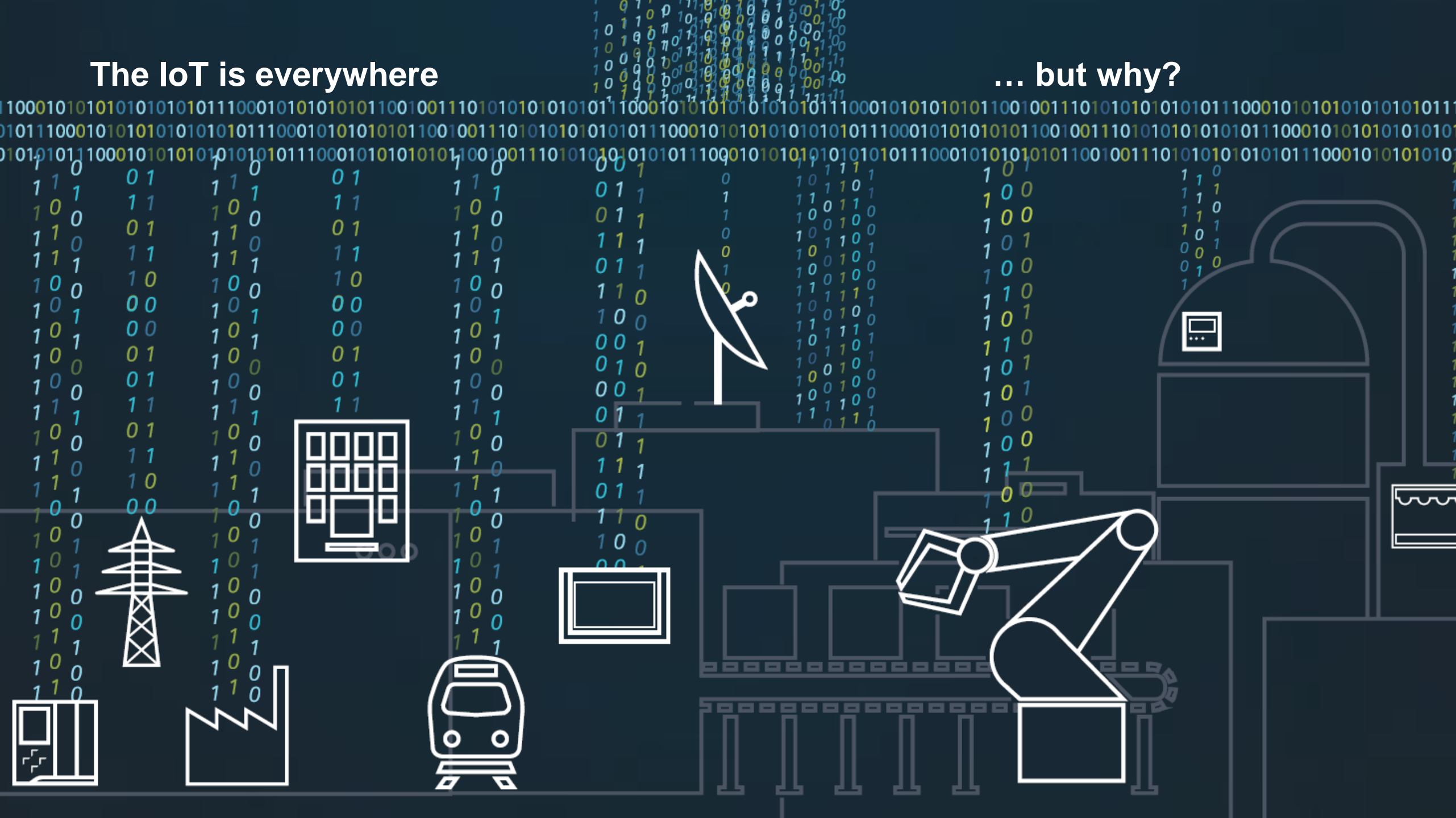


IoT Security – A joint approach



The IoT is everywhere

... but why?



Connectivity & Digitalization help your business



Accessible healthcare

- software simulations and real-time integration in diagnostic imaging
- automation systems handling and analyzing large amounts of patient data
- robotics in sample management and analysis

Smart cities

- intelligent building automation systems
- integrated mobility solutions
- smart-grid technologies
- security and crisis management

Future of manufacturing

- automated optimization of drives
- software simulations and integrations
- energy efficiency
- additive manufacturing

Some key players in IoT security...

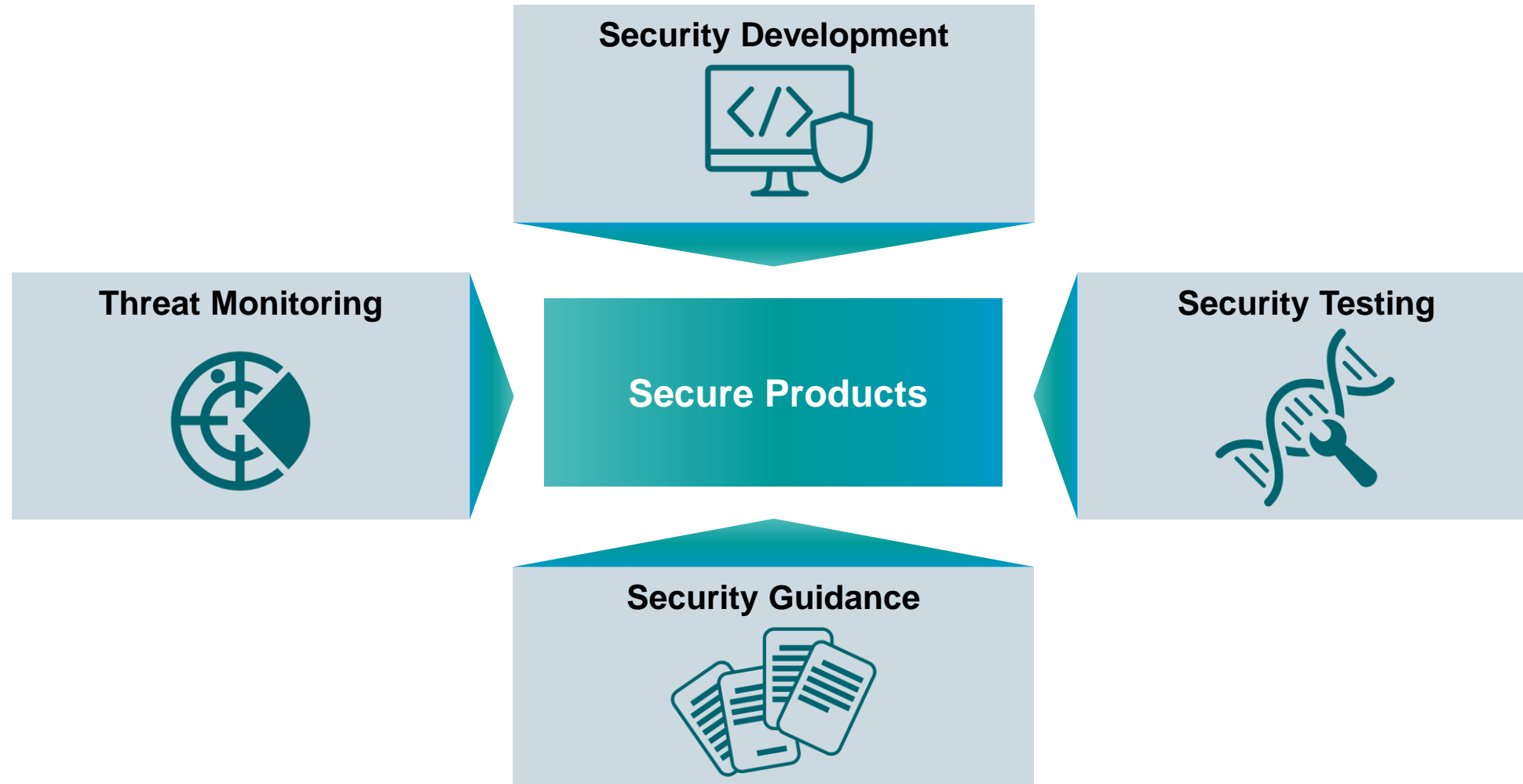


...and all of them are responsible for their own domain!

The role of the vendor



How vendors supply secure products



Roles of CSIRT & PSIRT

CSIRT

A computer security incident response team (CSIRT) is a concrete organizational entity (i.e., one or more staff) that is assigned the responsibility for coordinating and supporting the response to a computer security event or incident. CSIRTs can be created for nation states or economies, governments, commercial organizations, educational institutions, and even non-profit entities. The goal of a CSIRT is to minimize and control the damage resulting from incidents, provide effective guidance for response and recovery activities, and work to prevent future incidents from happening. (US-CERT.GOV)

PSIRT

A Product Security Incident Response Team (PSIRT) is an entity within an organization which, at its core, focuses on the identification, assessment and disposition of the risks associated with security vulnerabilities within the products, including offerings, solutions, components and/or services, which an organization produces and/or sells. (FIRST.ORG)

Security needs a holistic approach

CorporateCERT

- Incident Response in Large Scale Enterprise Environments
- Outstanding Forensic Capabilities
- Large CERT Community Network
- Leading in Threat Intelligence
- FIRST Membership

CustomerCERT

Bringing Experience Together, Creating Synergies and Leveraging Knowledge



Unique Combination of Skills



Leveraging 20 years CERT experience



Process Excellence



Cross Domain Knowhow

ProductCERT

- Vulnerability Handling of Siemens Products and Solutions
- Close Contact to Security Researchers
- Close Contact to Industrial CERT Community

Protect our networks

Protect our customers' operations

Protect our products

The role of the researcher



Researcher help identify issues

Hall of Thanks

Siemens expresses its sincere thanks to all individuals ethically reporting security issues in Siemens' products, solutions, or services.

[Report a Security Issue](#)



Acknowledgements

Each name represents an individual or organization who has privately reported one or more security vulnerabilities in Siemens' products, solution, services, or infrastructure and worked with Siemens to mitigate the issue.

2018

Can Demirel
Biznet Bilisim

Melih Berk Eksioglu
Biznet Bilisim

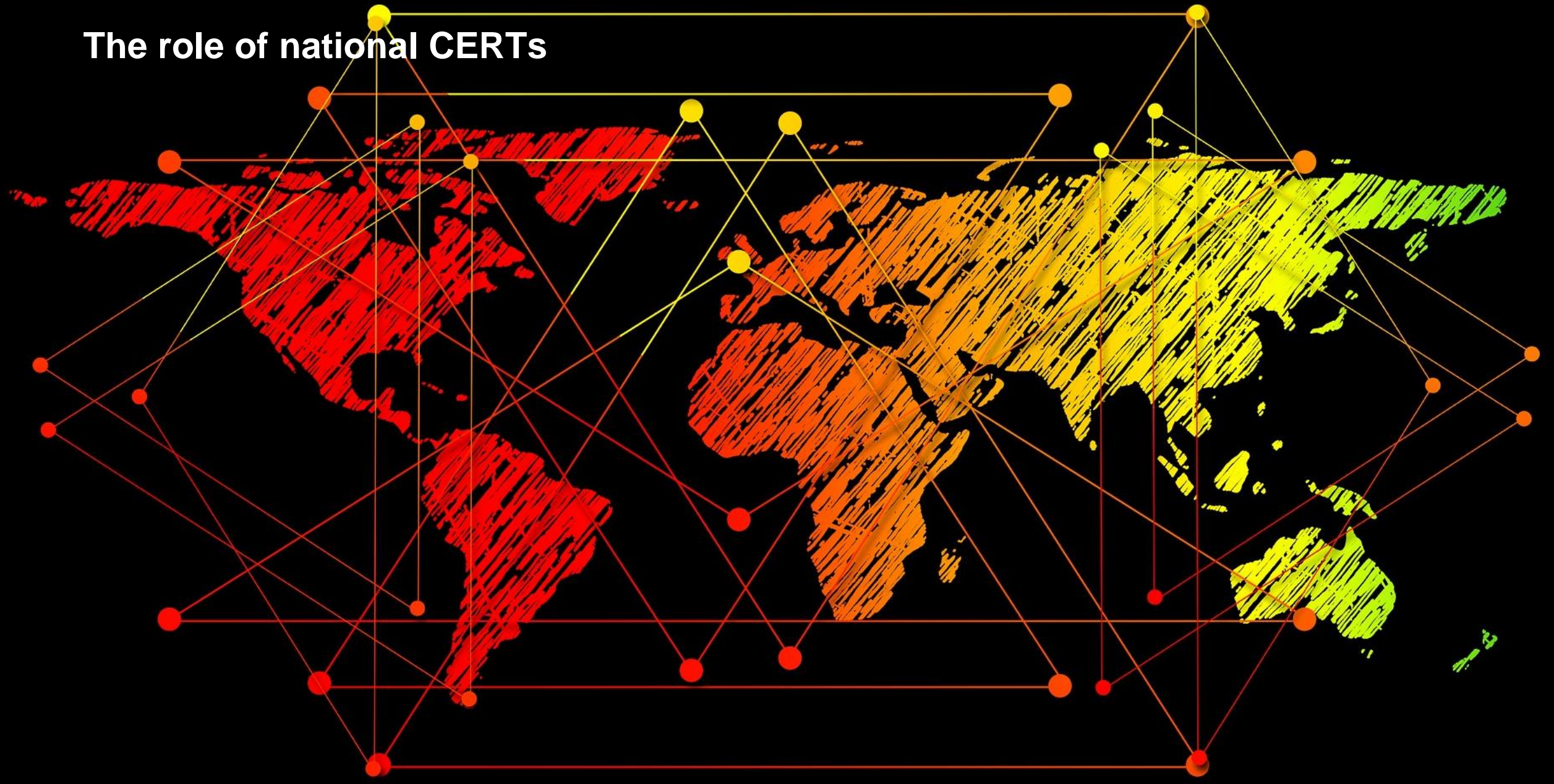
ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Can Demirel and Melih Berk Ekşioğlu from Biznet Bilişim for coordinated disclosure
- Industrial Control System Cyber Emergency Response Team (ICS-CERT) for coordination efforts

(example from recent Advisory)

The role of national CERTs



National CERTs and Coordination Teams

Vulnerabilities

- National CERTs are important contact points to researchers as they are independent from vendors.
- Vulnerability coordination teams facilitate a coordinated response amongst vendors affected by a shared issue (e.g. library).
- Advisory dissemination is an important task for national CERTs as they have the necessary channels and outreach to spread the word to operators.

Incidents

- National CERTs get informed about security related incidents within their realm and can create and share current threat information accordingly.
- National CERTs can leverage their authority to contact affected operators that would else go un-notified (e.g. through ISPs).

The role of the operator



Why is the operator so important?



Attackers Alter Water Treatment Systems in Utility Hack: Report

By [Eduard Kovacs](#) on March 22, 2016

They immediately noticed that the organization had a poor security architecture, with Internet-facing systems plagued by high-risk vulnerabilities known to be exploited in the wild, and outdated operation technology (OT) systems that had been more than ten years old.

NEWS

February 8, 2018 @ 7:19 AM

Industrial Control Systems Storm the Internet, Increase Corporate Risk

By [Douglas Bonderud](#)

U.S. Has Most Internet Connected Industrial Control Systems

By [SecurityWeek News](#) on July 11, 2016

AWDAM —

Vulnerable industrial controls directly connected to Internet? Why not?

Even some devices with patches available are connected to the naked Internet.

[SEAN GALLAGHER](#) - 1/26/2018, 1:11 AM

Defense-in-Depth strengthens the operator's posture



“**Defense in Depth** employs a holistic approach to protect all assets, while taking into consideration its interconnections and dependencies, and using an organization’s available resources to **provide effective layers** of monitoring and protection based on the business’s exposure to cybersecurity risks.”¹

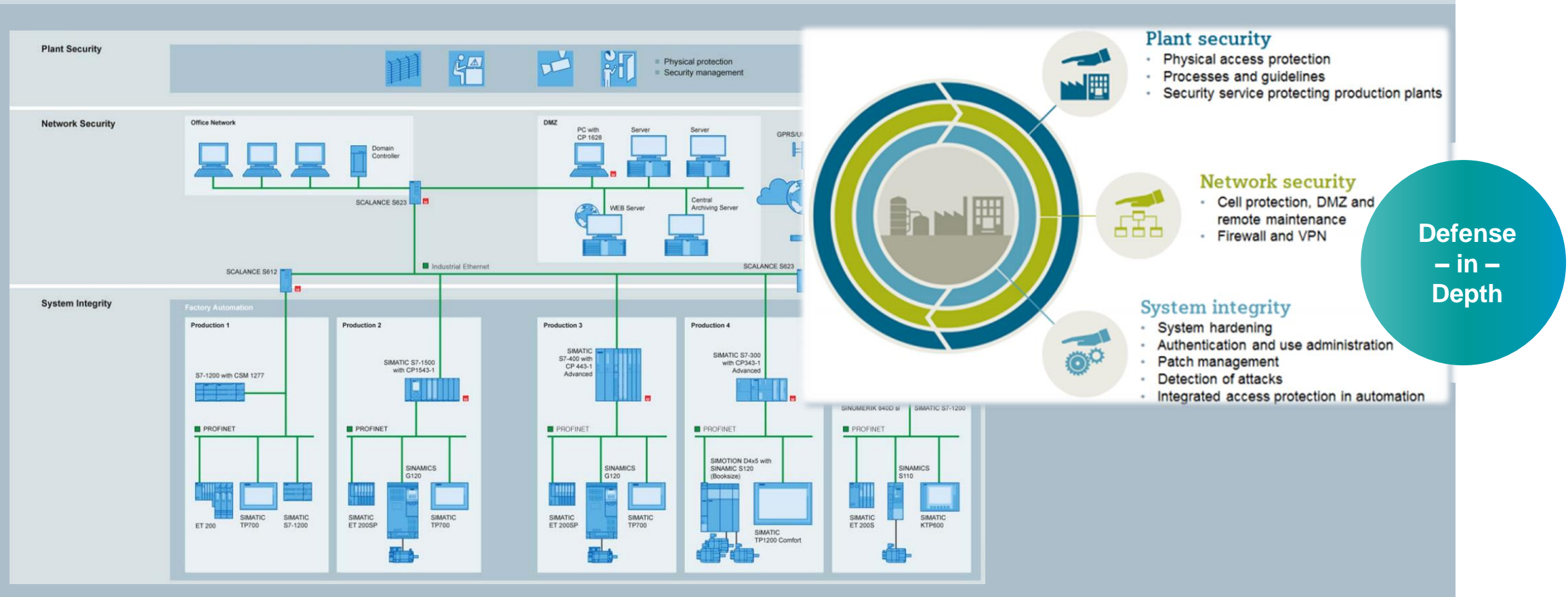
¹NCCIC, ICS-CERT, Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies, September 2016

Support by
Vendors
Available

Defense in Depth Strategy Elements	
Risk Management Program	<ul style="list-style-type: none"> Identify Threats Characterize Risk Maintain Asset Inventory
Cybersecurity Architecture	<ul style="list-style-type: none"> Standards/ Recommendations Policy Procedures
Physical Security	<ul style="list-style-type: none"> Field Electronics Locked Down Control Center Access Controls Remote Site Video, Access Controls, Barriers
ICS Network Architecture	<ul style="list-style-type: none"> Common Architectural Zones Demilitarized Zones (DMZ) Virtual LANs
ICS Network Perimeter Security	<ul style="list-style-type: none"> Firewalls/ One-Way Diodes Remote Access & Authentication Jump Servers/ Hosts
Host Security	<ul style="list-style-type: none"> Patch and Vulnerability Management Field Devices Virtual Machines
Security Monitoring	<ul style="list-style-type: none"> Intrusion Detection Systems Security Audit Logging Security Incident and Event Monitoring
Vendor Management	<ul style="list-style-type: none"> Supply Chain Management Managed Services/ Outsourcing Leveraging Cloud Services
The Human Element	<ul style="list-style-type: none"> Policies Procedures Training and Awareness

Example of Defense-in-Depth resources:

Digital Factory (Network Perspective)



Example of Defense-in-Depth resources:

Digital Factory (Device Perspective)



1	Minimizing Risk through Security	4
1.1	Security strategies	4
1.2	Implementation of strategies into solutions	5
1.2.1	Strengthening the sense of responsibility	5
1.2.2	The Siemens protection concept: "Defense in Depth"	6
1.3	Differences between office security and industrial security	7
1.4	Differences between functional safety and industrial security	7
1.5	Security management	8
2	Security Mechanisms of the S7 CPU	9
2.1	Block protection	9
2.2	Online access and function restrictions	12
2.3	Copy protection (S7-1200 (V4) / S7-1500).....	13
2.4	Local access protection (S7-1500).....	14
2.5	Further measures for protecting the CPU	15
3	Security Mechanisms of the S7-CPs	17
3.1	Stateful Inspection Firewall	17
3.2	Data encoding via VPN	18
3.3	NAT/NAPT (address translation).....	18
3.4	Secure IT functions	19
3.4.1	File Transfer Protocol (FTP).....	19
3.4.2	Network Time Protocol (NTP)	19
3.4.3	Hypertext Transfer Protocol (HTTP)	20
3.4.4	Simple Network Management Protocol (SNMP).....	20
4	The Achilles Certification Program	21



Example of Defense-in-Depth resources:

Energy Management

SIEMENS

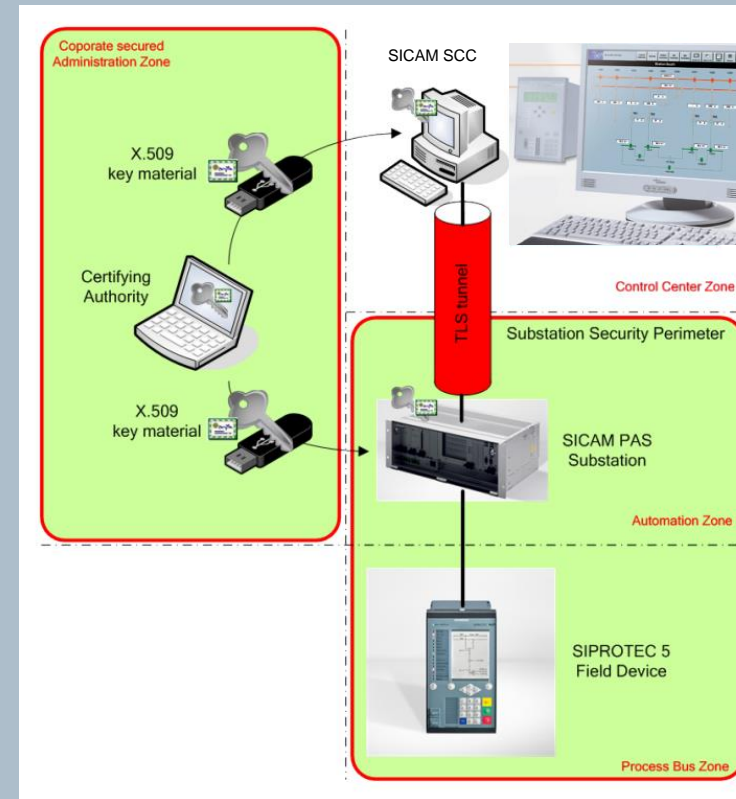
SICAM/SIPROTEC

System Hardening for Substation Automation and Protection

V1.11

Guideline (Best-Practice Guide)

Introduction	1
Network Security	2
User Management	3
Logging	4
Intrusion Detection System (IDS) - Snort	5
Malware Protection/Prevention	6
Hardening	7
Annex	8



Defense
– in –
Depth

Example of Defense-in-Depth resources:

Building Technologies

<p>SIEMENS</p>  <p>Siveillance Vantage™ IT Security Guide Engineering</p>	<p>SIEMENS</p>  <p>Mass Notification Security Concepts Version 2.1 Operation Manual</p>	<p>SIEMENS</p>  <p>SIPOINT MP3.0 Access Control System IT Security Operation Manual</p>
---	---	---

Contents

1	Introduction	7
1.1	Categorization of Measures	7
1.2	Security Requirement Categories.....	8
1.2.1	Security Requirement Category "Normal".....	8
1.2.2	Security Requirement Category "High".....	8
1.2.3	Security Requirement Category "Very High".....	9
2	Safety	10
2.1	Target Group.....	10
2.2	Work Safety Information	10
2.3	Hazard Symbols Defined	10
3	System Structure	11
3.1	Segmentation	11
3.2	Open System.....	12
3.3	Logically Contained System.....	13
3.4	Contained System	14
4	Security Measures	15
4.1	General Measures	15
4.1.1	Authentication	15
4.1.2	Password Guidelines	15
4.1.3	Biometric Authentication.....	15
4.1.4	No Use of Wireless Input Devices	15
4.1.5	Remote Maintenance.....	16
4.1.6	Time Synchronization.....	16
4.1.7	System Update	16
4.1.8	Deactivation of Guest and Unused Access.....	16
4.2	Network.....	17
4.3	Virtual Machines	17
4.4	Servers.....	17
4.4.1	Physical Protection of Interfaces	17
4.4.2	BIOS Settings and Passwords	18
4.4.3	Password Protection for Boot Manager	18
4.4.4	Use of the Kernel's Security Measures	18
4.4.5	Deactivation of Core Dumps.....	19

**Defense
– in –
Depth**

Cybersecurity – A critical factor for the success of the digital economy

KEY PRINCIPLES

Charter of Trust for a secure digital world

charter-of-trust.com

1. Ownership of cyber and IT security

Anchor the responsibility for cybersecurity at the highest governmental and business levels by designating specific ministries and CISOs. Establish clear measures and targets as well as the right mindset throughout organizations – “It is everyone’s task”.

2. Responsibility throughout the digital supply chain

Companies – and if necessary – governments must establish risk-based rules that ensure adequate protection across all IoT layers with clearly defined and mandatory requirements. Ensure confidentiality, authenticity, integrity, and availability by setting baseline standards, such as

- **Identity and access management:** Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.
- **Encryption:** Connected devices must ensure confidentiality for data storage and transmission purposes, wherever appropriate.
- **Continuous protection:** Companies must offer updates, upgrades, and patches throughout a reasonable lifecycle for their products, systems, and services via a secure update mechanism.

3. Security by default

Adopt the highest appropriate level of security and data protection and ensure that it is pre-configured into the design of products, functionalities, processes, technologies, operations, architectures, and business models.

4. User-centricity

Serve as a trusted partner throughout a reasonable lifecycle, providing products, systems, and services as well as guidance based on the customer’s cybersecurity needs, impacts, and risks.

5. Innovation and co-creation

Combine domain know-how and deepen a joint understanding between firms and policymakers of cybersecurity requirements and rules in order to continuously innovate and adapt cybersecurity measures to new threats; drive and encourage i.a. contractual Public Private Partnerships.

6. Education

Include dedicated cybersecurity courses in school curricula – as degree courses in universities, professional education, and trainings – in order to lead the transformation of skills and job profiles needed for the future.

7. Certification for critical infrastructure and solutions

Companies and – if necessary – governments establish mandatory independent third-party certifications (based on future-proof definitions, where life and limb is at risk in particular) for critical infrastructure as well as critical IoT solutions.

8. Transparency and response

Participate in an industrial cybersecurity network in order to share new insights, information on incidents et al.; report incidents beyond today’s practice which is focusing on critical infrastructure.

9. Regulatory framework

Promote multilateral collaborations in regulation and standardization to set a level playing field matching the global reach of WTO; inclusion of rules for cybersecurity into Free Trade Agreements (FTAs).

10. Joint initiatives

Drive joint initiatives including all relevant stakeholders in order to implement the above principles in the various parts of the digital world without undue delay.

Thank You!
**For keeping our communities
safe and secure!**